Załącznik nr 2 do zapytania ofertowego

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

Wykaz czynności związanych z kompleksową obsługa informatyczną RDOŚ w Rzeszowie oraz Wydziałów Spraw Terenowych w Krośnie i w Przemyślu (70 pracowników)

1. Instalacja, serwis oprogramowania zakupionego przez Zamawiającego z wyjątkiem przypadków wymagających interwencji dostawcy oprogramowania, zgodnie z poniżej zamieszczonymi zasadami:
   1) Wykonawca dokonuje instalacji wskazanego oprogramowania na stacjach roboczych i serwerach wskazanych przez Zamawiającego,
   2) Zamawiający dostarczy Wykonawcy nośniki instalacyjne, lub wskaże ich źródło, oraz dostarczy dokumenty poświadczające posiadanie licencji na instalowane oprogramowanie,
   3) serwis oprogramowania, który nie wymaga interwencji jego autora polega na:
      a) usuwaniu usterek w działaniu programów, które nie wymagają interwencji autora,
      b) nadzorowaniu poprawności wykonywanych kopii bezpieczeństwa baz danych programów,
      c) wykonywaniu instalacji nie wymagających obecności autora, nowych wersji oprogramowania oraz jego zmodyfikowanych wersji tzw. *Upgrade,*
      d) dostosowywaniu środowiska systemu operacyjnego komputerów do stanu umożliwiającego, poprawną instalację oprogramowania, tylko w przypadku, gdy nie jest w takiej sytuacji, konieczna interwencja autora oprogramowania,
      e) informowaniu Zamawiającego o stwierdzonych nieprawidłowościach w funkcjonowaniu wykorzystywanych przez niego programach,
      f) nadzorowaniu instalacji wszelkich modyfikacji oprogramowania wykonywanych przez pracowników autora oprogramowania,
      g) kontaktowaniu się z autorem oprogramowania w przypadku wystąpienia awarii, w celu jak najszybszego jej usunięcia.
2. Konserwacja i serwis sieci komputerowych wykorzystywanych przez Zamawiającego zgodnie z poniżej zamieszczonymi zasadami za wyjątkiem przypadków, w których naprawa musi być wykonana przez autoryzowany serwis:
   1) Wykonawca nadzoruje poprawność działania sieci komputerowej i w razie awarii podejmuje kroki zmierzające do jej usunięcia własnymi siłami. W koniecznych przypadkach wzywa serwis zewnętrzny za zgodą Zamawiającego,
   2) Wykonawca podłącza/odłącza od sieci komputerowej urządzenia wskazane przez Zamawiającego (posiadające interfejs RJ45),
   3) Wykonawca wykonuje konfigurację urządzeń sieciowych (posiadających interfejs RJ45) dostosowując ich sposób działania do potrzeb Zamawiającego.
3. Serwis sprzętu komputerowego za wyjątkiem przypadków, w których czynność serwisowa musi być wykonana przez autoryzowaną firmę zewnętrzna, zgodnie z poniżej

zamieszczonymi zasadami:

1) Wykonawca prowadzi naprawy sprzętu komputerowego, które nie wymagają interwencji autoryzowanego serwisu, za wyjątkiem sprzętu objętego gwarancją producenta, który nie podlega żadnym naprawom realizowanym przez Wykonawcę z wyłączeniem przypadków zgody producenta i pisemnej akceptacji Zamawiającego,
2) wszystkie podzespoły konieczne do naprawy realizowanej przez Wykonawcę dostarczy Zamawiający,
3) wszelkie podzespoły sprzętu komputerowego, które pozostaną po wykonanej naprawie Wykonawca przekaże Zamawiającemu wraz z informacją z jakiego sprzętu pochodzą,
4) wszystkie czynności serwisowe na sprzęcie komputerowym Zamawiającego będą wykonywane ze starannością gwarantującą zabezpieczenie przechowywanych tam danych.

4. Administrowanie serwerami Zamawiającego, a w szczególności:
   1) monitorowanie stanu serwerów i usuwanie wszelkich nieprawidłowości w ich pracy,
   2) zarządzanie kontami użytkowników na administrowanych serwerach,
   3) wykonywanie kopii bezpieczeństwa danych przechowywanych na serwerach,
   4) instalowanie i konfigurowanie nowych serwerów na użytek Zamawiającego,
   5) odtwarzanie serwerów po awarii – system operacyjny, oprogramowanie, dane.
5. Pomoc przy prowadzonych przez Zamawiającego postępowaniach przetargowych, a w szczególności:
   1) opracowywanie specyfikacji technicznych na kupowany sprzęt komputerowy i oprogramowanie,
   2) ocenianie złożonych ofert pod kątem ich zgodności technicznej z wymogami SIWZ.
6. Współpraca z informatykami Generalnej Dyrekcji Ochrony Środowiska lub odpowiednich Ministerstw w zakresie obsługi informatycznej, w tym udział w spotkaniach organizowanych przez ww. jednostki.
7. Zapewnienie sprawności i funkcjonalności systemów informatycznych w Regionalnej Dyrekcji, w których przetwarzane są dane osobowe,
8. Nadzorowanie funkcjonowania poszczególnych systemów, w których przetwarzane są dane osobowe, w szczególności w zakresie zarządzania prawami dostępu do tych systemów, oraz przeciwdziałaniu nieuprawnionemu dostępowi do systemów, a także podejmowaniem odpowiednich działań w przypadku wykrycia naruszeń tych systemów.
9. Usługi będą wykonywane w możliwie krótkim czasie nie dłuższym jak poniżej:

Parametr	**Wartość**
Czas reakcji na zgłoszenie	do 1,5 godziny
Czas usunięcia błędu krytycznego	do 1 dnia roboczego
Czas usunięcia błędu poważnego	do 2 dni roboczych
Czas usunięcia błędu uciążliwego	do 5 dni roboczych

8. W jednym dniu w tygodniu ustalonym pomiędzy Zamawiającym i Wykonawcą, przedstawiciel Wykonawcy będzie pełnił dyżur w siedzibie Zamawiającego od godziny. 9.00 do 15.30.
9. W przypadku wprowadzenia jednego ze stopni alarmowych CRP (ALFA CRP, BRAVO CRP, CHARLIE CRP lub DELTA CRP) Wykonawca zapewni realizację przedsięwzięć wymienionych w *Rozporządzeniu Prezesa Rady Ministrów z dnia 25 lipca 2016 r. w sprawie zakresu przedsięwzięć wykonywanych w poszczególnych stopniach alarmowych i stopniach alarmowych CRP* (Dz. U z 2016 r. poz. 1101) a w szczególności:

1) wprowadzi zwiększoną kontrolę stanu bezpieczeństwa systemów teleinformatycznych, a w szczególności:
   a) będzie monitorował i weryfikował, czy nie doszło do naruszenia bezpieczeństwa komunikacji elektronicznej,
   b) będzie sprawdzał dostępność usług elektronicznych,
   c) będzie dokonywał, w razie potrzeby, zmian w dostępie do systemów,
2) poinformuje własny personel (w szczególności odpowiedzialnych za bezpieczeństwo systemów) o konieczności zachowania zwiększonej czujności w stosunku do stanów/sytuacji odbiegających od normy,
3) sprawdzi kanały łączności z innymi podmiotami biorącymi udział w reagowaniu kryzysowym jak również dokona weryfikacji ustanowionych punktów kontaktowych z podmiotami reagowania na incydenty bezpieczeństwa teleinformatycznego,
4) dokona przeglądu procedur oraz zadań związanych z wprowadzaniem stopni alarmowych CRP, a w szczególności:
   a) zweryfikuje posiadane kopie zapasowe systemów w stosunku do systemów teleinformatycznych wchodzących w skład infrastruktury krytycznej oraz systemów kluczowych dla funkcjonowania RDOŚ,
   b) zweryfikuje czas wymagany na przewrócenie poprawności funkcjonowania sytemu,
5) sprawdzi aktualny stan bezpieczeństwa systemów i oceni wpływ zagrożenia na bezpieczeństwo teleinformatyczne na podstawie bieżących informacji i prognoz wydarzeń,
6) będzie Informował na bieżąco o efektach przeprowadzonych działań zespoły reagowania na incydenty bezpieczeństwa,
7) zapewni dostępność w trybie alarmowym personelu odpowiedzialnego za bezpieczeństwo systemów,
8) wprowadzi całodobowy dyżur administratorów systemów kluczowych dla funkcjonowania RDOŚ oraz personelu uprawnionego do podejmowania decyzji w sprawach bezpieczeństwa systemów teleinformatycznych,
9) dokona przeglądu dostępnych zasobów zapasowych pod względem możliwości wykorzystania w przypadku zaistnienia ataku,
10) przygotuje się do uruchomienia planów umożliwiających zachowanie ciągłości działania po wystąpieniu potencjalnego ataku, w tym min.:
    a) dokona przeglądu i ewentualnego audytu planów awaryjnych oraz infrastruktury teleinformatycznej, w tym wyznaczy systemy kluczowe do utrzymania ciągłości pracy,
    b) przygotuje się do ograniczenia operacji na serwerach, w celu możliwości ich szybkiego i bezawaryjnego zamknięcia, pozostawi dostęp wyłącznie użytkownikom wytypowanym przez administratora.